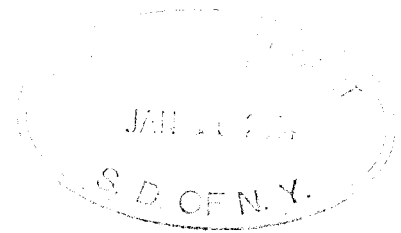


ORIGINAL

Approved:


EUN YOUNG CHOI/JAMES PASTORE
Assistant United States Attorneys

Before: THE HONORABLE RONALD L. ELLIS
United States Magistrate Judge
Southern District of New York



-----X
UNITED STATES OF AMERICA : SEALED **14 MAG 0108**
: COMPLAINT
:
-v- : Violations of 18 U.S.C.
: §§ 2251(a), (e),
MARK ANTHONY WARREN, : 2252A(a)(2), 875(d), and
: 2.
Defendant. :
: COUNTY OF OFFENSES:
-----X NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

DOC #

JOHN ROBERTSON, being duly sworn, deposes and says that she is a Special Agent with the Federal Bureau of Investigations ("FBI") and charges as follows:

COUNT ONE

(Production of Depiction of Sexually Explicit Conduct Involving a Minor)

1. From at least November 2013, up to and including in or about about December 2013, in the Southern District of New York and elsewhere, MARK ANTHONY WARREN, the defendant, knowingly did employ, use, persuade, induce, entice, and coerce a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct and for the purpose of transmitting a live visual depiction of such conduct, and did know and have reason to know that such visual depiction would be transported and transmitted using a means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce, and such visual depiction was transported and transmitted using a means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce, to wit, WARREN induced a minor in the Southern District of New York to engage in sexually explicit conduct, which WARREN secretly recorded by video and transmitted through

the Internet from Australia to the Southern District of New York.

(Title 18, United States Code, Sections 2251(a) and 2.)

COUNT TWO

(Attempted Production of Depiction of Sexually Explicit Conduct Involving a Minor)

2. From at least November 2013, up to and including in or about December 2013, in the Southern District of New York and elsewhere, MARK ANTHONY WARREN, the defendant, knowingly attempted to employ, use, persuade, induce, entice, and coerce a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct and for the purpose of transmitting a live visual depiction of such conduct, and did know and have reason to know that such visual depiction would be transported and transmitted using a means and facility of interstate and foreign commerce and in and affecting interstate or foreign commerce, and that such visual depiction would be transported and transmitted using a means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce, to wit, WARREN attempted to persuade, induce, entice, and coerce a minor in the Southern District of New York into creating a video of that minor engaging in sexually explicit conduct and then transmitting that video through the Internet to WARREN in Australia.

(Title 18, United States Code, Sections 2251(a), (e) and 2).

COUNT THREE

(Receipt and Distribution of Child Pornography)

3. From at least in or about November 2013 up to and including in or about December 2013, in the Southern District of New York and elsewhere, MARK ANTHONY WARREN, the defendant, knowingly did produce, receive and distribute a visual depiction of a minor engaging in sexually explicit conduct, which was shipped and transported in and affecting interstate and foreign commerce, and which contained materials which were so shipped and transported, by means including by computer, and knowingly did reproduce such a visual depiction for distribution using a means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce, to wit, WARREN knowingly received, and caused to be distributed and received, videos depicting child pornography, including a video of a minor

engaging in sexually explicit conduct in the Southern District of New York.

(Title 18, United States Code, Section 2252A(a)(2) and 2.)

COUNT FOUR
(Extortion)

4. During at least in or about December 2013, in the Southern District of New York and elsewhere, MARK ANTHONY WARREN, the defendant, with intent to extort from a person, money and another thing of value, knowingly did transmit in interstate and foreign commerce a communication containing a threat to injure the property and reputation of the addressee and of another and a threat to accuse the addressee and any other person of a crime, to wit, through internet messages transmitted from Australia to the Southern District of New York, WARREN threatened to publicly embarrass and humiliate a minor, and to wrongly accuse that minor of committing a crime, in order to coerce that minor into engaging in sexually explicit conduct on video and transmitting that video from the Southern District of New York to Australia.

(Title 18, United States Code, Section 875(d).)

The bases for my knowledge and for the foregoing charges are as follows:

5. I am a Special Agent with FBI, and I have been personally involved in the investigation of this matter. I have been assigned to the Crimes Against Children Squad, which investigates, among other things, the sexual exploitation of children in violation of Title 18, United States Code, Sections 2251 and 2252A. I am familiar with the information contained in this Complaint based on my own personal participation in the investigation, my review of documents, conversations I have had with other law enforcement officers about this matter, my training and experience, and numerous discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Because this Complaint is being submitted for the limited purpose of establishing probable cause to arrest the defendant, I have not included the details of every aspect of the investigation. Where actions, conversations, and statements of others are related herein, they are related in substance and in part, except where otherwise indicated. In addition, all dates and times contained herein are approximate, and have been converted

to Eastern Standard Time ("EST") for ease of reference, unless otherwise noted.

Definitions

6. The following terms have the indicated meaning in this Complaint:

a. The terms "minor," "sexually explicit conduct," and "visual depiction," as used herein, are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "child pornography," as used herein, is a visual depiction of a minor involved in sexually explicit conduct as defined in Title 18, United States Code, Section 2256(8).

Overview

7. As detailed below, from at least in or about November 2013 up to and including in or about December 2013, MARK ANTHONY WARREN, the defendant, has used multiple false identities and posed on the Internet as a teenage girl in order to trick, coerce, and extort minor male victims into producing child pornography at his direction.

8. In particular, MARK ANTHONY WARREN, the defendant, created bogus accounts on various social media websites using false identities and posing as various teenage girls and a teenage boy. WARREN contacted male minors, including a 14-year-old in New York, New York, and, posing as a teenage girl, engaged them in sexually explicit discussions via web chats. During the web chats, WARREN secretly recorded the minor males engaging in sexually explicit conduct. After making these secret recordings of his minor victims, WARREN contacted them again and threatened to publish the videos to the victims' families and friends unless the victims created additional pornographic videos of themselves and uploaded them to a particular website accessible by WARREN. WARREN provided the victims with specific, detailed instructions about the sexually explicit videos they were to make at his direction. WARREN also told his victims that he used particular methods to obscure his identity and was beyond the reach of law enforcement.

Background on the Internet

9. Based on my training and experience gained from this case and others, I know that every computer or device on the Internet has an Internet protocol or "IP" address assigned to it, which is used to route Internet traffic to or from the device. A computer's or a device's IP address can be used to determine its physical location and, thereby, its user. Individuals engaged in criminal activity on the Internet, including individuals engaged in child exploitation and child pornography, use means designed to facilitate anonymity of their computers and devices, and thereby, their locations and identities. These means include the following:

a. Proxy Servers: Proxy servers, including virtual private network ("VPN") servers, act as intermediate, secure gateways through which users can remotely login to various online accounts or computers. Proxy servers redirect communications from the user to the target website or computer, such that the user's IP address is only shared with the proxy server, and the target website or computer can only see the proxy server's information.

b. The Tor Network: "The Onion Router" or "Tor" network ("Tor") is a special network of computers on the Internet, distributed around the world, that is designed to conceal the user's true IP addresses. Communications sent through Tor are bounced through numerous relays within the network, and then subject to encryption, such that it is practically impossible to trace the communication back to its true originating IP address.

10. Based on my training and experience, I also know that there are ways to identify individuals who use the above-referenced means of hiding their location and identity. For example:

a. Individuals who know how to anonymize their presence on the Internet often choose not to do so, especially when they are not engaged in illicit activities. Thus, individuals may reveal their true IP addresses by logging onto websites directly, without the use of either a proxy server or Tor.

b. Certain websites and programs, including many social media sites, use various means and methods to identify individual users of the website, including by retaining data that identifies whether a particular computer or electronic

device has been used to access different accounts or webpages within a particular website.

The Investigation

11. I have spoken with an individual ("Victim-1"), and reviewed documents provided by Victim-1, and have learned, in substance and in part, the following:

a. Victim-1 is a 14-year-old male who lives in New York, New York.

b. On the evening of December 12, 2013, Victim-1 accessed a particular social media website which connects users at random for the purpose of engaging in real-time communications ("chats") by text and video with each other (the "Real-Time Site"). On the Real-Time Site, Victim-1 engaged in sexually explicit text chats with an individual who claimed to be a teenage girl named "Amy." Thereafter, Victim-1 engaged in sexually explicit conduct over a video chat with "Amy," while "Amy" also purported to be engaged in sexually explicit conduct.

c. Later that evening, "Amy" provided to Victim-1 a link to an account on a particular social media website (the "Social Media Website") in which "Amy" was identified by purported first and last name (the "Amy Social Media Account"). Through the Amy Social Media Account, Victim-1 engaged in a series of communications with "Amy."

d. Several hours later, Victim-1 received an electronic message from the Amy Social Media Account that included a link and access password to a video that "Amy" had uploaded to a particular website which enables users to share video content with others (the "Video Website"). Victim-1 subsequently viewed the video which, to Victim-1's surprise, depicted Victim-1 engaged in sexually explicit conduct during his real-time communications with "Amy" on the Real-Time Site. Accompanying the video on the Video Website was a threat written in the comments section associated with the video which stated that the video would be distributed to Victim-1's friends and relatives unless Victim-1 followed "Amy's" instructions. In particular, it stated, among other things:

A small part of a much bigger video. Would be a shame if all your friends and family were sent a link via [the Social Media Website] to the whole movie.

To make sure the movie isn't seen by anyone else all you have to do is record 5 private videos. After that your off the hook.

Warning - don't tell anyone about this. Your parents will be horrified, ban you from doing anymore videos and stop you using the computer. I will then send the link out. The police cannot track me as I cloak my identity with TOR (google it) and I am in a country with no extradition arrangements with the US anyway. Also - if you go to the police you will likely be charged with child pornography - both downloading and uploading (again google teen sexting). You will have a criminal record and be forever registered as a sex offender. At the same time and all your friends will still see your video. . . .

From now on email me at [an email address with the same purported first and last name as the Amy Social Media Account ("Amy Email Address")] to receive instructions.

. . . Just do the simple videos that I ask and your movies will never been seen by anyone else. Fuck with me though and I will send the links.

e. Victim-1 then received a series of messages from the Amy Social Media Account instructing him to send an email to the Amy Email Address, and also specifying precisely what videos he was supposed to create, and how he was to transmit them. The messages included specific instructions about the nature of the sexually explicit videos Victim-1 was to create.

12. On or about December 14, 2013, at or about 8:20 PM, a Social Media account in the first and last name of a particular purported individual (the "Danny Social Media Account") sent Victim-1 the following electronic message, which I reviewed:

You don't know me but I see you are a [Social Media Website] friend of Amy [last name redacted] (I am too). I know this sounds strange but I was wondering if you knew her in real life not just thru [the Social Media Website]?? I'd really appreciate it if you could let me know ASAP as I need to sort something out with her.

13. I have spoken with an employee of the Social Media Website ("Social Media Employee"), and reviewed records provided

by the Social Media Website, and have learned, in substance and in part:

a. The Amy Social Media Account was created on or about November 14, 2013, and its user provided the Amy Email Address to the Social Media Website as the email address associated with the user.

b. On or about November 30, 2013, the Amy Social Media Account was used to contact another individual on the Social Media Website ("Victim-2"). Thereafter, through the Amy Social Media Account, "Amy" sent Victim-2 the following message:

Hi [Victim-2]. This is a shitty message to write cause I know what you are about to feel. You have been caught out on cam by a sick fuck. He tricked u with a fake video and recorded everything u did on cam and then friended u on [the Social Media Website]. He has now got all your friend details and he says he will post them all a link to your video if u dont do what he says. I'm messaging u because I was caught out too - he gets other guys in his trap to do his work for him.

I'm really sorry because I know how sick I felt when I got the same message a few weeks ago. Don't stress too much - from what Ive been told by other guys is that he keeps his word and if u cooperate he doesnt share the video.

He will get you to make some private videos for him - he promises after u do 5 your off the hook and wont hear from him again. I have done 3 so far and have been told what I have to do for the next one. He also told me to message you (I haven't spoken to him - this has come from another guy) and explain whats happening.

I'm really sorry dude - I know its shitty but I'm caught too. Please dont tell anyone! He says he cant be traced because he uses encryption and shit. All the logons to [the Social Media Website] etc are done by other kids so tracing them doesnt help and we all get caught. I cant fucking imagine what my life would be like if this got out. He says that if we go to the police we would get in trouble for broadcasting child porn. I googled it and its true. . . we get put on a sex register thing.

The videos are embarrassing to do but not too bad. I have sort of thought well he's seen me anyway so whats another video or 2 - as long as he doesnt show my family and friends. One of the guys that contacted me has said he did all the vids and none were shared so i'm trusting him - not sure what else to do anyway. I was told to tell you to delete this message so no-one sees it and from now on make contact using email to [Amy Email Address]. You have to send an email there to get your next instructions

Dude I'm really sorry to send this to you but I have no choice, .

If you want to talk to me email me privately I have set up a special email account for this shit (I suggest u do to so no one sees anything) - [email address containing the name "Danny"] (not my real name) I'll do my best to help you with this ok?

Finally I have to give you this link so you know he is serious . . . the password is [Victim-2's name]

[https://\[Video Website\].com/*****220](https://[Video Website].com/*****220)

Sorry I feel really bad - like i say u are going to feel like shit but dont freak too much - make sure you delete this so no one ever finds out. Also DONT unfriend him on [the Social Media Website]. He already has your friends bookmarked and if you unfriend him he will send a link to someone of your choice. One of the guys that emailed me had this happen - he had to tell him a friend to receive the link and he sent it. Just be cool and play along ok??

Email me when you can.

c. Thereafter, Victim-2 responded, in substance and in part, that he would not produce further videos despite these threats.

d. The next day, on December 1, 2013, "Amy" sent three separate electronic messages to Victim-2 through the Amy Social Media Account stating, in substance and in part, that Victim-2 should create additional videos or a particular video of Victim-2 would be disseminated. "Amy" further threatened, among other things, that "when he sends the video to everyone somebody will call the police for sure. . . that means you could

get charged with child porn. . . . Im also guessing if this does get to the police we will all be found. . . . so all of us will get charged. . . ."

e. On or about December 10, 2013, Victim-2 received another series of electronic messages from the Amy Social Media Account which stated, among other things, "your [sic] the little bastard who didn't care if I showed his video to the world. Your [sic] lucky that I wouldn't ever do that to a kid. . . ."

"Mark Warren" Accesses His Social Media Account and the Amy, Danny, and Other Bogus Social Media Accounts to Contact Minors

14. In my analysis and review of Social Media records, I have learned that since its creation, the Amy Social Media Account has been accessed from a number of different IP addresses, including IP addresses that I believe, based on my experience and review of databases containing IP information, to stem from proxy servers and the Tor Network which, as set forth above, are used in an effort to mask the true location of the user.

15. Despite the fact that many of the IP addresses that have accessed the Amy Social Media Account appear to stem from proxy servers and the Tor Network, I have learned several pieces of information about them from my review of Social Media records. In particular, as forth below, the same small set of IP addresses has variously accessed a small set of Social Media accounts, including an account in the name of "Mark Warren" (the "Mark Warren Social Media Account"), the Amy Social Media Account, the Danny Social Media Account, and accounts in the purported first and last name of three other individuals (the "Emily Social Media Account," the "Emma Social Media Account," and the "Grace Social Media Account"), often in close temporal proximity. This group of IP addresses includes one IP Address that I believe to be an IP address that has not been anonymized, as well as various IP addresses that stem from proxy services and the Tor Network. Based on my review, all these Social Media accounts with the exception of one – the Mark Warren Social Media Account – appear to be bogus accounts used to induce and attempt to induce minor males to engage in sexually explicit conduct.

The 245 IP Address

16. Based on my review of Social Media records, I have learned that from in or about May 2013 through and including December 2013, the Mark Warren Social Media Account was accessed over 400 times from a particular IP address ending in 245 ("245 IP Address"). The 245 IP Address has also been used to access:

a. the Amy Social Media Account, which was accessed from the 245 IP Address on or about December 2, 2013 at approximately 7:40 PM. Notably, the Mark Warren Social Media Account was accessed later that evening, on or about December 3, 2013, at approximately 2:59 AM, also from the 245 IP Address. The Amy Social Media Account was also accessed from the 245 IP Address approximately three times on or about November 24, 2013 and approximately three times on or about December 14, 2013.

b. the Danny Social Media Account, which was accessed from the 245 IP Address on or about December 14, 2013 at approximately 8:17 PM – just prior to the message that was sent from that account to Victim-1, in which "Danny" asked Victim-1 if he knew "Amy" "in real life not just thru Social Media??" as described above in Paragraph 12. After this question was sent to Victim-1, the 245 IP Address accessed the Danny Social Media Account approximately three more times that same evening, December 14, 2013.

c. the Emily Social Media Account, which was accessed from the 245 IP Address on or about November 9, 2013 at approximately 4:43 PM, less than two hours after that account was created.

The 131 IP Address

17. From my review of Social Media records, I have learned that the Mark Warren Social Media Account has also been accessed from a particular IP address ending in 131 (the "131 IP Address") which, based on my review, has also been used to access certain interrelated Social Media accounts, as follows:

a. On or about November 9, 2013 at approximately 2:10 AM, the 131 IP Address was used to access the Mark Warren Social Media Account.

b. One minute later, at approximately 2:11 AM, the 131 IP Address was used to create the Emma Social Media Account, which features the purported photograph of "Emma," who (based on my review) appears to be a teenage girl.

Other IP Addresses

18. From my review of Social Media records, I have learned the following:

a. On or about November 9, 2013, at approximately 3:15 AM, the Emily Social Media Account was created. Based on my review, the photograph of "Emily" featured in the Emily Social Media Account appears to be identical to the photograph of "Emma" featured in the Emma Social Media Account, which, as described in the previous section, had been created less than two hours before.

b. On or about November 10, 2013, the Mark Warren Social Media Account was accessed from a particular IP address ending in 633 (the "633 IP Address") at approximately 12:22 AM. Minutes earlier, at approximately 12:11 AM, the 633 IP Address accessed the Emily Social Media Account.

c. On or about November 12, 2013 at approximately 7:08 PM, the Grace Social Media Account was created using an IP address ending in 129 (the "129 IP Address"). On or about November 14, 2013, at approximately 3:32 AM, the Grace Social Media Account was accessed from the 129 IP Address. A few minutes later, at approximately 3:34 AM, the 129 IP Address was used to access the Emily Social Media Account.

d. On or about November 14, 2013 at approximately 1:00 AM, the Mark Warren Social Media Account was accessed from an IP address ending in 123. About a minute later, at approximately 1:01 AM, the Grace Social Media Account was accessed from the same IP address.

e. On or about November 15, 2013, at approximately 7:41 AM, the Amy Social Media Account was accessed from an IP address ending in 130. Approximately a minute later, at 7:42 AM, the Emily Social Media Account was accessed from that same IP address.

Use of Same Computers or Electronic Devices

19. From my review of Social Media records, I have learned that the same computers or electronic devices that have accessed the Mark Warner Social Media Account have also accessed the Amy, Grace, and Emily Social Media Accounts. Specifically:

a. From on or about November 14, 2013 at approximately 12:25 AM to on or about November 15, 2013 at 8:03 AM, the same computer or electronic device was used to access the Mark Warren Social Media Account, and the Grace and Emily Social Media Accounts.

b. From on or about November 20, 2013 at approximately 10:29 PM to November 21, 2013 at approximately 3:37 AM, the Mark Warner Social Media Account was accessed from a particular computer or electronic device. On or about November 24, 2013 at approximately 4:54 PM, that same computer or electronic device was used to access the Amy Social Media Account.

c. On or about November 24, 2013 at approximately 7:53 PM, the Amy Social Media Account was accessed from a particular computer or electronic device. A few minutes later, at approximately 7:55 PM, that same computer or electronic device was used to access the Mark Warren Social Media Account.

Use of Bogus Social Media Accounts to Contact Minors

20. I have reviewed Social Media records reflecting the activities of the Emma, Emily, and Grace Social Media Accounts. From that review, I learned, in substance and in part, that these accounts have been used to contact Social Media account users that appear, based on photographs and content on those accounts, to be minor males, and in some instances, to discuss engaging in real-time video communications and exchanging photographs.

Video Depictions of Sexually Explicit Conduct
Were Uploaded to the Video Website

21. I have spoken with a Video Website employee ("Video Website Employee"), and reviewed records obtained from the Video Website, and have learned the following, in substance and in part:

a. A Video Website user with the same purported first and last name as "Amy" (from the Amy Social Media Account) has uploaded three videos to the Video Website. The date and time, and IP address from which the clip was uploaded to Video Website, and the clip number are as follows:

Video	Date/Approx. Time	IP Address	Clip ¹
1	12/12/2013 10:36 PM	An IP address ending in 969	*****686
2	11/30/2013 11:07 PM	An IP address ending in 432	*****220
3	11/24/2013 6:12 AM	An IP address ending in 120	*****312

b. I have reviewed Video 1, Video 2, and Video 3. Video 1 is the pornographic video of Victim-1 described above in Paragraph 11(d). Video 2 depicts a minor male, and contains child pornography, and Video 3 depicts a teenage male engaged in sexually explicit conduct, although from the video alone I cannot determine conclusively whether he is a minor.

c. The clip number *****686 associated with Video 1 matches the website URL that was provided to Victim-1 by "Amy," as described above in Paragraph 11(d), i.e., [https://\[Video Website\].com/*****686](https://[Video Website].com/*****686).

d. The clip number *****220 associated with Video 2 matches the website URL that was provided to Victim-2 by "Amy," as described above in Paragraph 13(b), i.e., [https://\[Video Website\].com/*****220](https://[Video Website].com/*****220).

e. In addition to depicting a teenage male engaging in sexually explicit conduct, Video 3 contains a banner of text

¹ The full numbers for these video clips have been edited to reflect only the last three numbers.

that scrolls across the top of the video continuously throughout the video's duration. The text provides:

Surprise. This is NOT a joke. You have 24HRs to email [Amy Email Address] otherwise EVERYONE on your [Social Media] friends list will get a download link to the full high quality version of your performance on cam. Do NOT tell anyone about this as nobody can help. I cannot be tracked as I use lots of technogy [sic] to hide my online presence. The police are powerless - they cannot even tell what country I am from. The only thing that will happen is YOU will be charged with child pornography and will be recorded on a sex offender register for life. Do NOT panic too much though. This is easily fixed with no-one ver [sic] knowing or seeing your performance except you and I. Again email [Amy Email Address] within 24 hours for instructions. Do NOT delete me from Social Media . I have bookmarked ALL your friends and will send them this video if you do not co-operate in full. You have 24 hours from now - [Amy Email Address].

The User of the Mark Warren Social Media Account is
MARK ANTHONY WARREN, the Defendant

22. From my review of Social Media records, I have learned, in substance and in part, the following regarding the Mark Warren Social Media Account:

a. The Mark Warren Social Media Account was created in July 2012. Mark Warren presents himself on the Social Media account as an adult male born in 1965, who lives in or around Sydney, Australia. From my review of the contents of the Mark Warren Social Media Account, I know that Mark Warren has or had a wife ("Warren's Wife"). Messages on the Mark Warren Social Media Account state that he is soliciting work in the media industry, and that he is working as a consultant and recruiter in the media industry.

b. On or about December 6, 2013, the Mark Warren Social Media Account uploaded a photograph. Social Media records retain the approximate geographic location (latitude and longitude) of where the photograph was taken, which I have determined, using Google Maps, to be in the vicinity of the intersection of two streets ("Street-1" and "Street-2"), in Neutral Bay, New South Wales, Australia. Neutral Bay appears to be a suburb located North of Sydney.

c. Mark Warren provided two email addresses ("Email-1" and "Email-2") to the Social Media Website.

23. From publicly available databases and sources, I have learned the following:

a. An online resume of Mark Warren states that Warren lives in the greater Sydney area and works in the media industry. It also states that he has run a media consulting company ("Company-1") since March 2013, and that he was previously a publisher at another media company ("Company-3").

b. The website of Company-1 lists Mark Warren as a consultant based in Sydney, and has the same domain name as that of Email-1, i.e., one of the email addresses provided by Mark Warren to the Social Media Website.

c. The website for a recruiting company ("Company-2"), lists Mark Warren as a consultant for the New South Wales area, and has a link to Email-2.

d. The website for Company-3 confirms that Mark Warren previously worked at Company-3, along with Warren's Wife.

24. In an effort to identify and confirm the individual responsible for the above described crimes, I have provided to Australian law enforcement authorities information I have learned and collected over the course of my investigation, including a picture of "Mark Warren" from the Mark Warren Social Media Account.

25. I have spoken with a member of the Australian Federal Police ("AFP Officer") who has told me, in substance and in part, that the 245 IP Address, from which the Mark Warren Social Media Account was accessed over 400 times, is subscribed to in the name of Warren's Wife, with a physical address on Street-1 in Neutral Bay, New South Wales, Australia ("Warren House"), i.e., the same street in the vicinity of which the photograph described above in Paragraph 22(b) was taken.

26. I have spoken with an FBI agent assigned as an Assistant Legal Attaché in Australia ("FBI ALAT") who, in turn, has spoken with a member of the New South Wales Police Force ("NSW Officer"), and I have reviewed a report prepared by the New South Wales Police Force, from which I have learned, in substance and in part, the following:

a. On January 16, 2014 at approximately 1:44 PM Australian Eastern Daylight Time, Australian law enforcement agents executed a search warrant at the Warren House based on information provided by the FBI. While agents were executing the search warrant, an individual arrived at the Warren House and identified himself as "Mark Warren."

b. Australian law enforcement agents identified "Mark Warren" as MARK ANTHONY WARREN, the defendant, born in 1965.

c. MARK ANTHONY WARREN, the defendant, identified to agents various electronic devices, including an external hard drive, as belonging to him, and admitted that he was sexually attracted to male minors.

d. Australian law enforcement agents, in executing the search warrant at the Warren House, performed a preliminary review of the external hard drive of MARK ANTHONY WARREN, the defendant, and found images that appeared to depict minors engaged in sexually explicit conduct.

WHEREFORE, the deponent respectfully requests that an arrest warrant be issued for MARK ANTHONY WARREN, the defendant, and that he be arrested and imprisoned, or bailed, as the case may be.



JOHN ROBERTSON
Special Agent
Federal Bureau of Investigations

Sworn to before me this
16th day of January, 2014



THE HONORABLE RONALD L. ELLIS
United States Magistrate Judge
Southern District of New York